



Administrator Manual

For Convene 3.8.x (Web), Convene 4.0.1082 (Android), Convene 4.0.10928 (iPad)
Manual Version: 20141218R1



Table of Contents

Mobile App Installation and Sign In	3	Folder and File Permissions	27
iPad	3	Grant Permissions	27
Android	8	Revoke Permissions.....	28
Accessing the Portal.....	13	Audit Trail	29
Manage User Accounts	14	System Administration	30
Create User Accounts	14	License	34
Enable / Disable User Accounts	15	Meeting Types	35
Manage Users from an LDAP Server	15	System Key.....	36
Reset User Password.....	16		
Erase Mobile App Data.....	17		
Manage Roles and Permissions	18		
User Roles and Permissions	18		
Meeting Roles and Permissions	20		
Manage Groups	24		
Create a Group.....	24		
Add Members.....	25		
Remove Members.....	26		



Mobile App Installation and Sign In iPad

Install from Appstore

1. Using your iPad or iPhone, launch the **App Store** application.
2. Search for **Azeus Convene**.
3. Install **Azeus Convene**.





Mobile App Installation and Sign In (iPad) Advanced Server Configuration

Convene can connect to Convene Portal behind a firewall by opening the required ports directly in the firewall or using a proxy server that has support for HTTP and SOCKS version 5.

The following ports are required by Convene to connect to the portal:

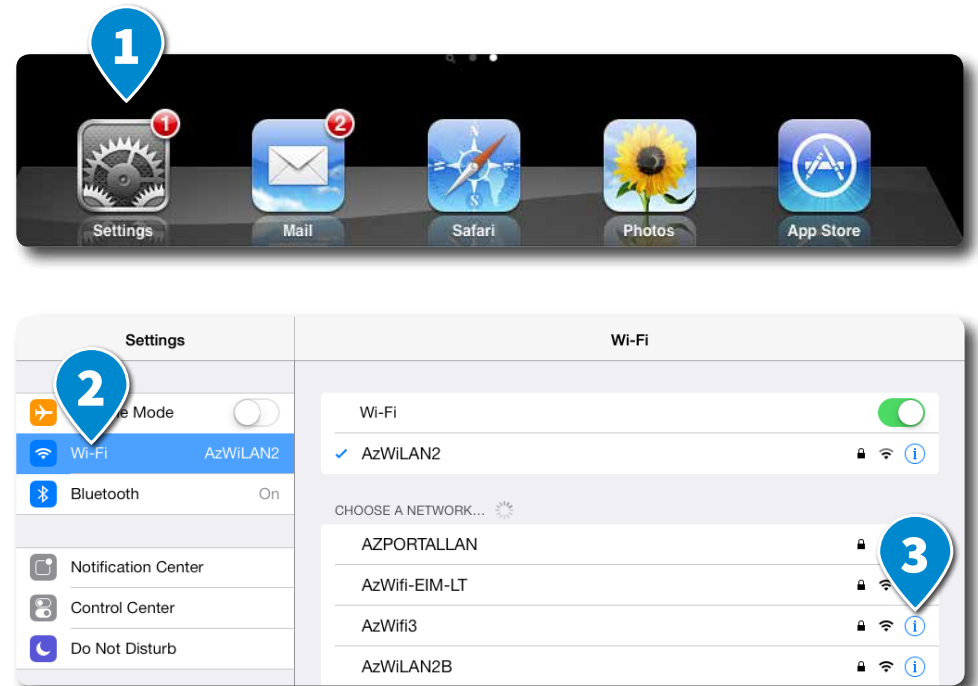
- 80
- 443

iPad Proxy Configuration

HTTP Proxy Configuration

To allow Convene to use a proxy server with HTTP support, configure the iPad network settings by following these steps:

1. Launch **iPad Settings**.
2. Tap **Wi-Fi**.
3. Tap ⓘ to open the **Wi-Fi settings**.





Mobile App Installation and Sign In (iPad)

Advanced Server Configuration

4. Go to the **Manual** tab under the **HTTP PROXY** section and configure the following parameters:

Parameter	Values
Server	required, either host name or IP address
Port	required, proxy server listening port

If the proxy server specified requires authentication, slide the Authentication on and specify the Username and Password on the respective fields.





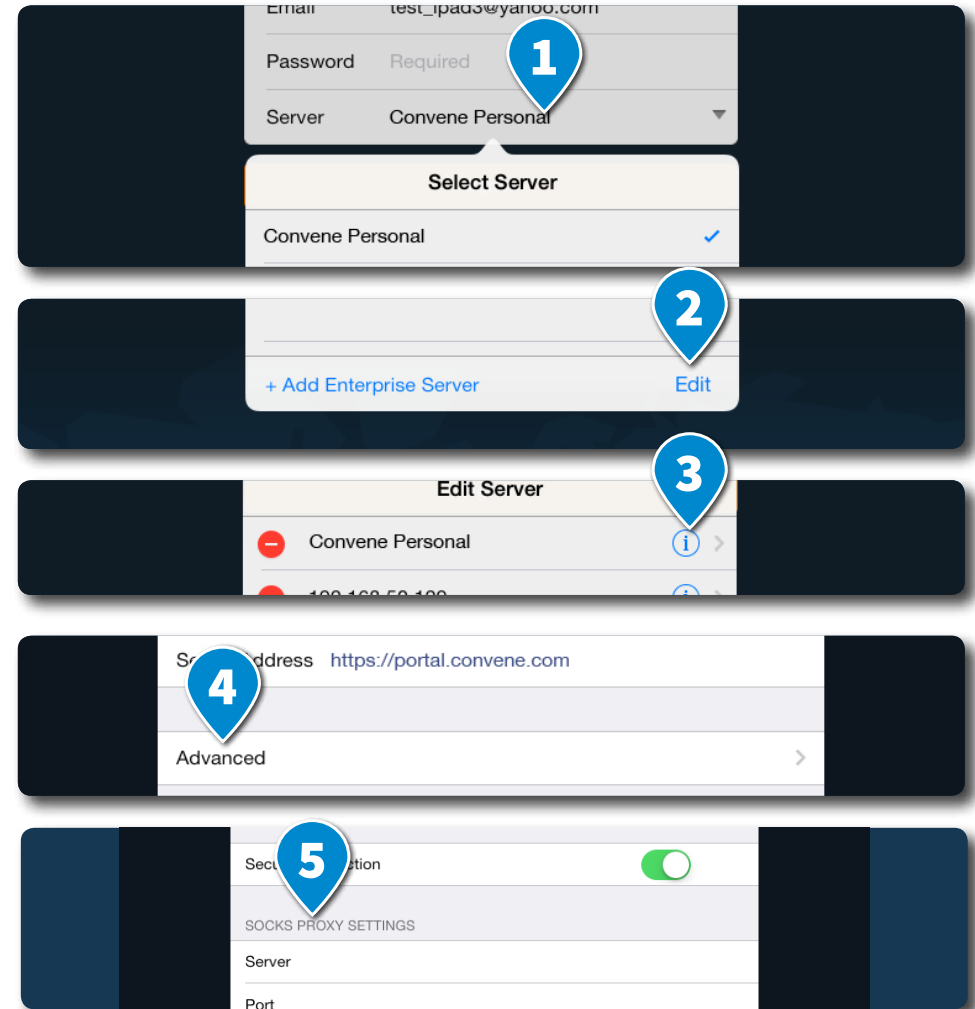
Mobile App Installation and Sign In (iPad)

Advanced Server Configuration

SOCKS Proxy Configuration

To configure Convene to use a proxy server with SOCKS version 5 support, follow these steps:

1. In the Convene sign in screen, tap **Server**.
2. Tap **Edit**.
3. Tap ⓘ on the server your want to configure.
4. Tap **Advanced**.
4. Under the **SOCKS Proxy Settings** section, fill-up the fields using values from your system administrator.

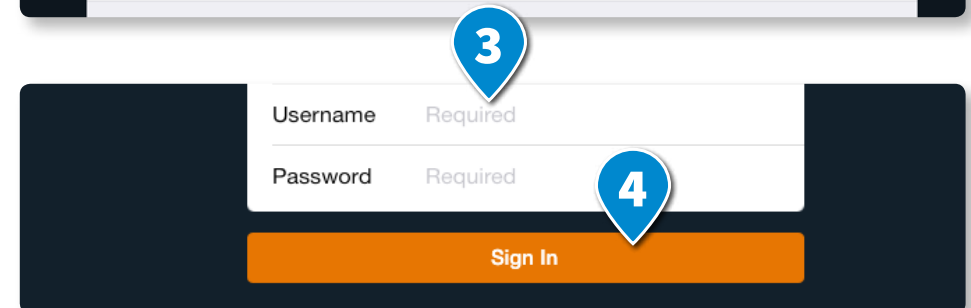
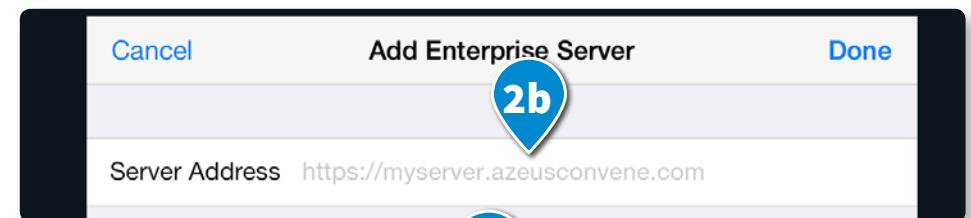
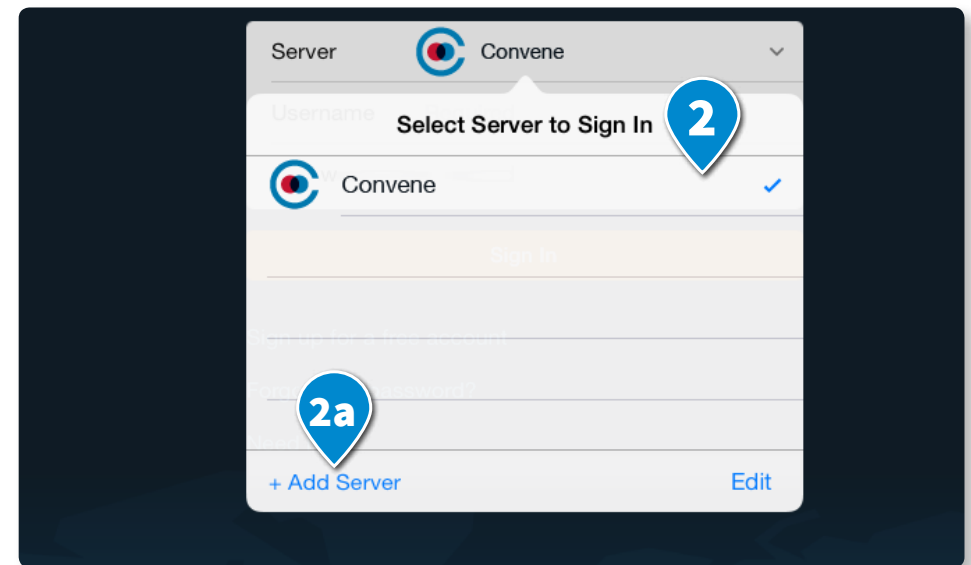




Mobile App Installation and Sign In (iPad)

Sign in to the Convene App

1. On your mobile device, tap the **Convene** icon.
2. (Optional) Specify the server to be used.
 - a) To add an enterprise server, tap **Add Server** from the Server dropdown.
 - b) On the Server Settings window, specify the **Server Address** and tap **Done**.
 - c) If multiple servers have been added, the next time you sign in, just tap **Server** and choose from the drop-down list which server to use for the current session.
3. Enter your **Username** or **Email** and **password**.
4. Tap **Sign in**.

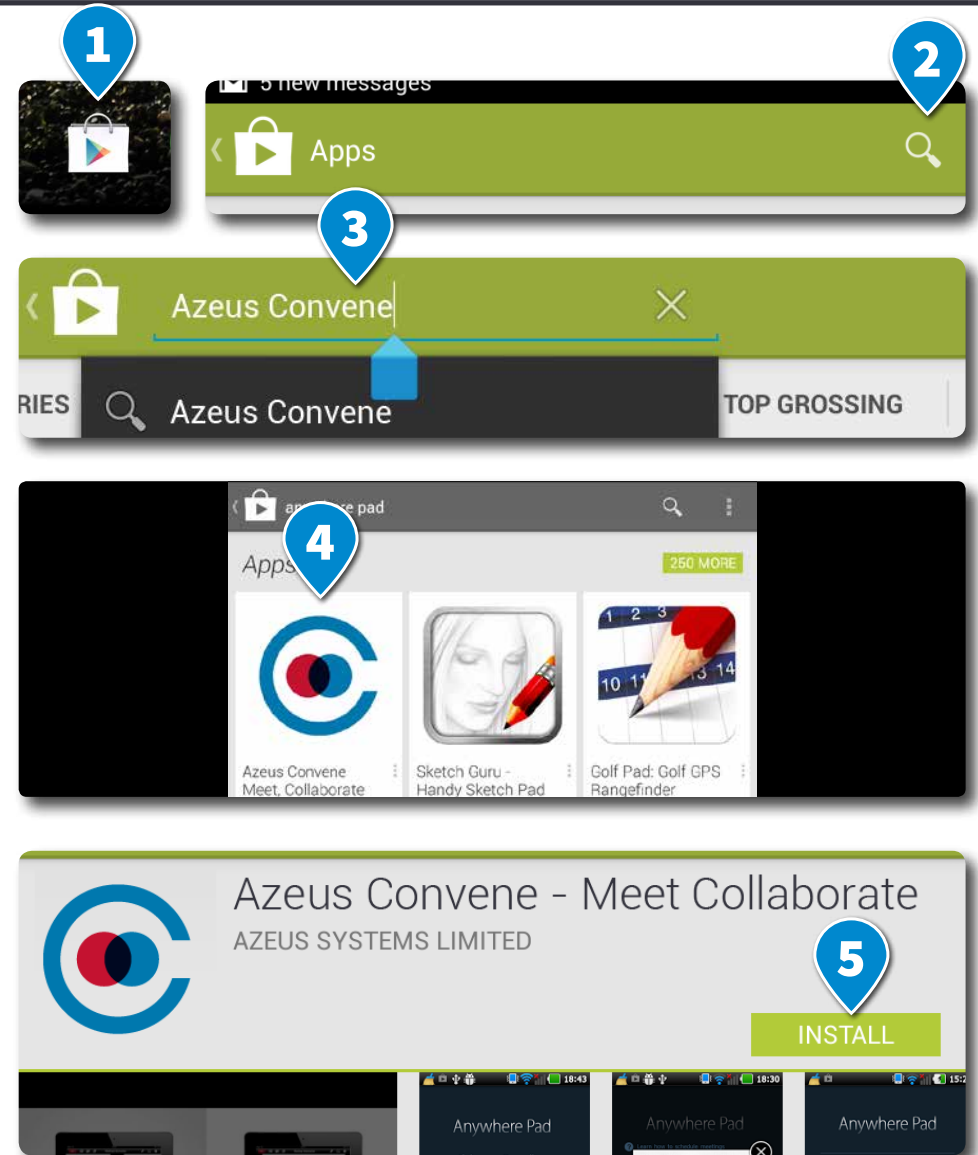




Mobile App Installation and Sign In Android

Install from Google Play Store

1. Using your Android device, launch the **Play Store** app.
2. Tap .
3. Type "Convene" and tap on .
4. Select **Convene** from the list.
5. Tap **Install**.
6. On the permissions dialog, tap **Accept**.





Mobile App Installation and Sign In (Android) Advanced Server Configuration

Convene can connect to Convene Portal behind a firewall by opening the required ports directly in the firewall or using a proxy server that has support for HTTP and SOCKS version 5 (Convene for Android also supports SOCKS version 4).

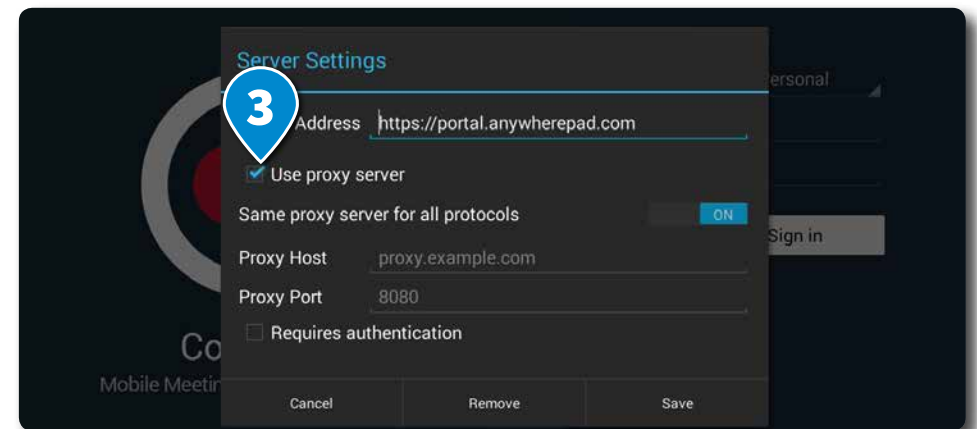
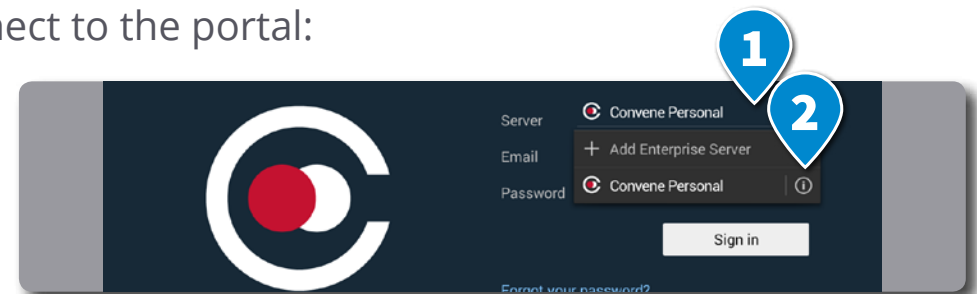
The following ports are required by Convene to connect to the portal:

- 80
- 443

Basic HTTP Proxy Configuration

To configure Convene to use a proxy server with HTTP support, follow these steps:

1. In the **Convene app** sign in screen, tap **Server**.
2. Tap ①.
3. Tick **Use Proxy Server** check box and specify the **Proxy Host** and **Proxy Port** on the respective fields.



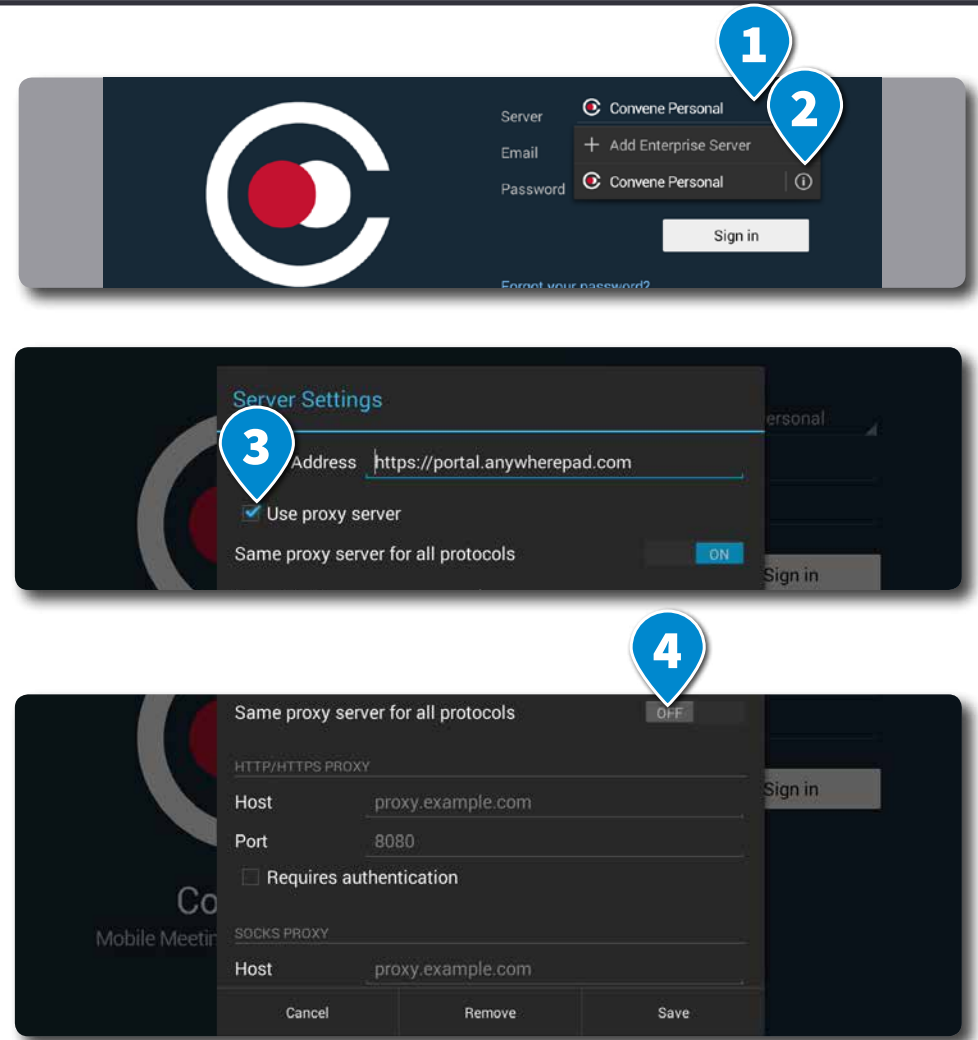


Mobile App Installation and Sign In (Android) Advanced Server Configuration

Advanced Proxy Configuration

To configure Convene to use specific proxy settings for HTTP, HTTPS and SOCKS version 4/5, follow these steps:

1. In the **Convene app** sign in screen, tap **Server**.
2. Tap ⓘ.
3. Tick **Use Proxy Server** and specify host name or IP address and port. This also applies to both HTTP and HTTPS.
4. Switch off **Same proxy for all protocols**.





Mobile App Installation and Sign In (Android)

Advanced Server Configuration

5. For each protocol, the user can configure the following parameters:

Parameter	Values
Host	required, either host name or IP address
Port	required, proxy host listening port

6. If the proxy host specified requires authentication, tick the **Requires Authentication** check box and configure the following parameters:

Parameter	Values
Username	optional, only if authentication is needed
Password	optional, only if authentication is needed

Server Settings

Server Address <https://portal.anywherepad.com>

☒ Use proxy server

Same proxy server for all protocols ☐ OFF

HTTP/HTTPS PROXY

Host 6

Port 5

☒ Requires authentication

Username

Password

SOCKS PROXY

Host

Port

☐ Requires authentication 7

Cancel Save

Note for SOCKS protocol:

- If **Username** is not specified, or if specified with the corresponding **Password**, SOCKS version 5 protocol will be used.
- If **Username** is specified without a **Password**, SOCKS version 4 protocol will be used.

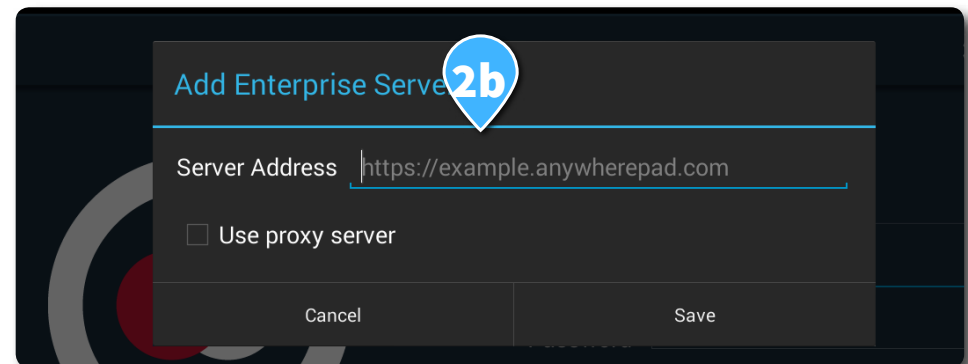
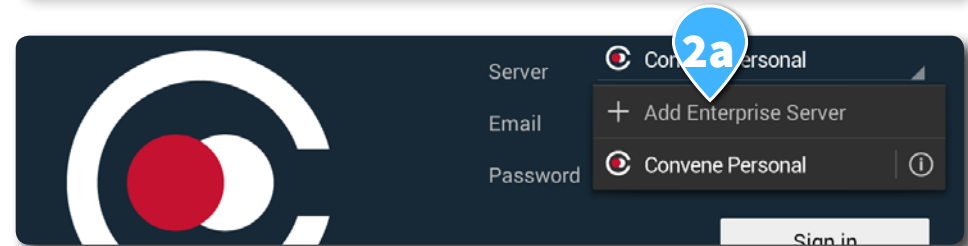
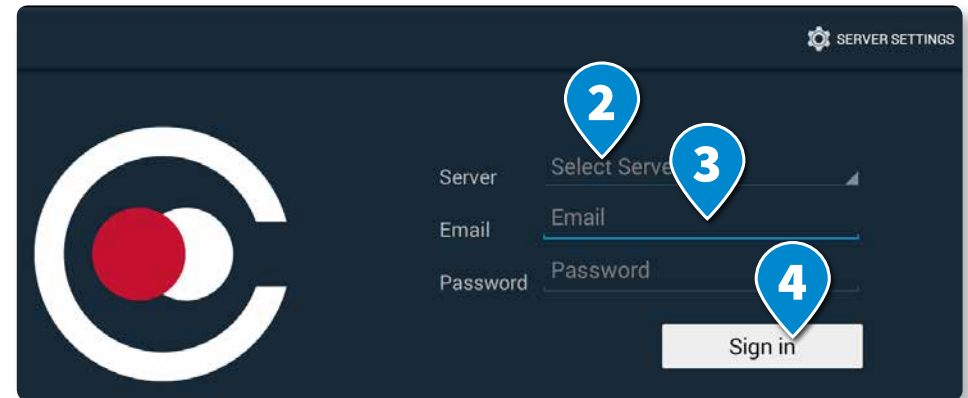
7. Tap **Save**.



Mobile App Installation and Sign In (Android)

Sign in to the Convene App

1. On your mobile device, tap the **Convene** icon.
2. Specify the server to be used.
 - a) To add an enterprise server, tap **Add Enterprise Server** from the Server dropdown.
 - b) On the Server Settings window, specify the **Server Address** and tap **Save**.
 - c) If multiple servers have been added, the next time you sign in, just tap **Server** and choose from the drop-down list which server to use for the current session.
3. Enter your **Username** or **Email** and **password**.
4. Tap **Sign in**.





Accessing the Portal

Introduction

The Convene web portal is a web-based application where you can change system settings, audit security logs, and perform administrative functions such as meeting management and user accounts management.

Accessing the Portal

You can access the portal using your PC's web browser. Please contact your administrator for the web address to use.

A mockup of a web portal's sign-in interface. It features a light blue header with the text "Sign In". Below the header, there are two input fields: "Username:" and "Password:". The "Username:" field is a simple text box, while the "Password:" field is a text box with a small eye icon on the right side. Below the "Password:" field, there is an orange button with the text "Sign in". To the right of the button, there is a link that says "Forgot password?". The entire form is enclosed in a blue border.

Sign In

Username:

Password:

Sign in

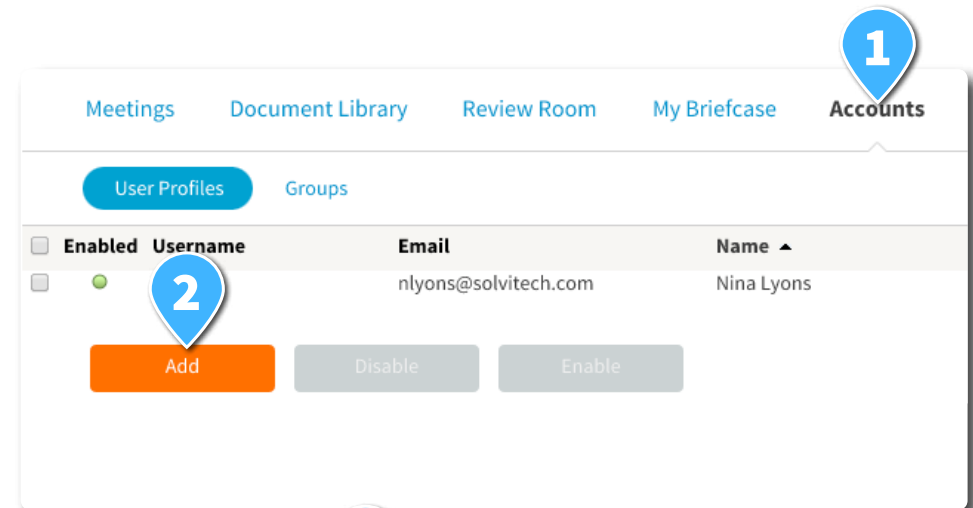
[Forgot password?](#)



Create User Accounts

Create User Accounts

1. Click on the **Accounts** tab.
2. Click **Add**.
3. On the **New User Profile** form, specify the appropriate fields. Please refer to the section **User Roles and Permission** for information about the Role field.
4. Click **Save and Close**.

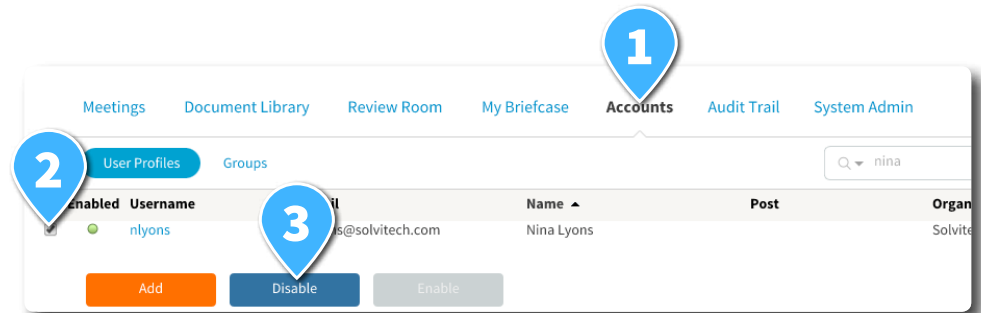




Enable/Disable User Accounts

Enable / Disable User Accounts

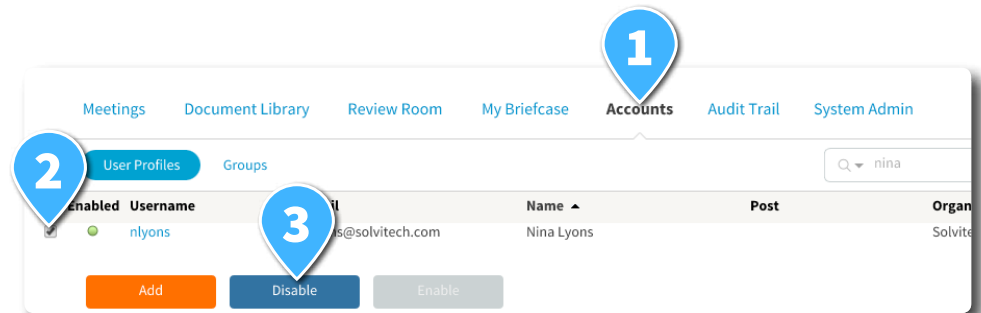
1. Click on **Accounts**.
2. Select the accounts you want to enable/disable.
3. Click the **Enable/Disable** button.



Manage Users from an LDAP Server

Accounts imported from an LDAP (Lightweight Directory Access Protocol) are disabled by default. To enable them:

1. Click on **Accounts**.
2. Select the accounts you want to enable.
3. Click the **Enable** button.





Reset User Password

Reset User Password

1. Under **Accounts**, click **User Profiles**.
2. Click on the **Username** of the account whose password you want to change.
3. Click **Change Password**.*
4. Specify a password for the account.
5. Retype the new password.
6. Click **Save and Close**. The system will prompt the user to change the account password upon sign in.

* For users that use ADFS authentication, this method cannot be used. The password should be reset through Active Directory.

© Copyright 2014. Azeus Systems Ltd. All rights reserved. This user manual may not be reproduced or distributed in whole or in part without prior permission from Azeus Systems Ltd. The content of this manual is intended for informational use only.

Accounts | Document Library | Review Room | My Briefcase | Accounts

User Profiles | Groups

Enabled	Username	Email	Name
☐	nlyons	nlyons@solvitech.com	Nina Lyons

Organisation: Solvitech

* Role: General User

Storage Limit: MB

Auto-download Briefcase Documents: Yes

Change Password | Erase Anywhere Pad Data | Save and Close | Cancel

Change Password

* New Password:

* Retype New Password:

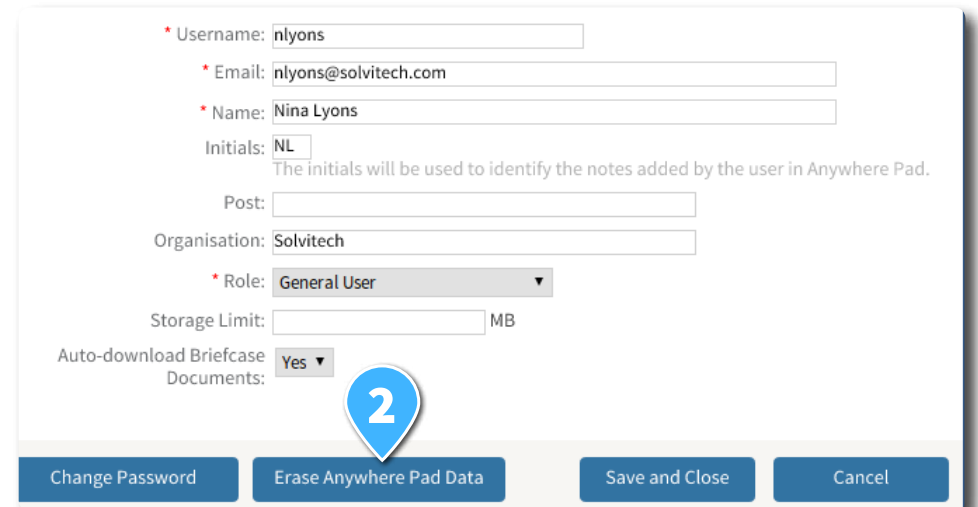
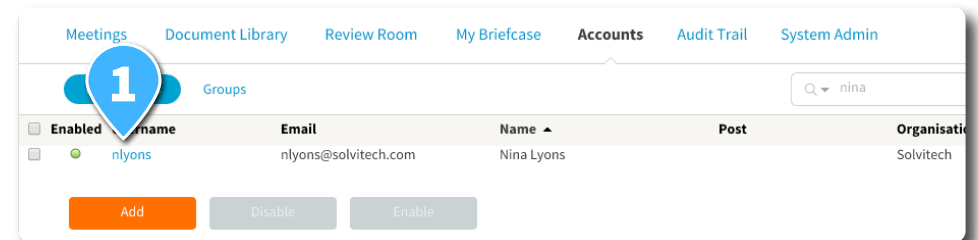
Save and Close | Cancel



Erase Mobile App Data

In case a device is lost or compromised, administrators can erase data on the device of a specified user.

1. Under **Accounts**, click on the **Username** of the user account whose mobile data you want to erase.
2. Click **Erase Convene App Data**.
3. Click **OK**.





User Roles and Permission

User Roles and Permissions

Convene maintains three user types with different levels of access. The table below shows the operations that can be performed by each type of user.

	General User	Administrator
Meeting Management		
Schedule/create meeting	Yes	Yes
Document Management		
Manage org-level folders	No	Yes
Set file and folder permission	Yes*	Yes

¹A General User can only manage a file or folder's access permissions if the user is granted administrative rights to that specific file or folder. Administrative rights to files or folders can only be granted a user who has administrative access to the same file or folder.



User Roles and Permission

	General User	Administrator
System Administration		
Manage accounts	No	Yes
Manage groups	No	Yes
Maintain corporate structure	No	Yes
View audit logs	No	Yes
Maintain meeting types	No	Yes
Maintain system settings	No	Yes



Meeting Roles and Permissions

Default Roles and Permissions

Convene has a number of built-in roles and permissions to help you get started right away. However, these roles can be customised as appropriate for your organisation.

CHAIRPERSON

The Chairperson role is intended for the user who will facilitate the meeting. A user with this role has all the permissions for the meeting:

- Manage meeting details, status and notifications
- Manage agenda and meeting files
- Manage participants
- Start and end meeting
- Download meeting files to desktop
- Export meeting pack
- Add shared annotations
- Add private annotations
- Assign presenter role during meeting
- Upload and manage meeting minutes
- Read all participants' private annotations
- Edit all participants' shared text notes after meeting



Meeting Roles and Permissions

SECRETARY

The secretary role has, by default, the same permissions as the Chairperson.

PARTICIPANT

A meeting participant can do the following:

- Download meeting files to desktop
- Add shared annotations
- Add private annotations

MEETING ORGANISER

By default, the Meeting Organiser is the user who scheduled the meeting, but other users may also be added as Meeting Organisers. Meeting Organiser(s) have the same permissions as the Chairperson except for the following:

- Read all participants' private annotations
- Edit all participants' shared text notes after meetings



Meeting Roles and Permissions

Although Convene provides a number of built-in meeting roles, you can customise these roles to reflect the roles and responsibilities within your organisation.

Add a Meeting Role

1. Click **System Admin**.
2. Go to **Meeting Roles** tab.
3. Click **Add New Meeting Role**.
4. Enter the name of the new role.
5. Specify what the role can do in a meeting by marking the corresponding checkboxes of function rights listed.
6. Click **Save and Close**.

The screenshot displays the Convene System Admin interface. At the top, the 'System Admin' tab is selected (1). Below it, the 'Meeting Roles' tab is chosen (2). A list of existing roles is shown, including Chairperson, Collaborator, Guest, Meeting Organiser, Observer, Participant, and Secretary (3). The 'Add New Meeting Role' button is highlighted. The form for adding a new role is shown below, with a 'Description' field (4). The 'Permission' section lists various functions with checkboxes (5). At the bottom, the 'Save and Close' button is highlighted (6).

Meeting Role
Chairperson
Collaborator
Guest
Meeting Organiser
Observer
Participant
Secretary

Add New Meeting Role **Delete Meeting Role(s)**

Description: *

Permission

Permission	Selected
Manage agenda and meeting files	☐
Download meeting files to desktop	☐

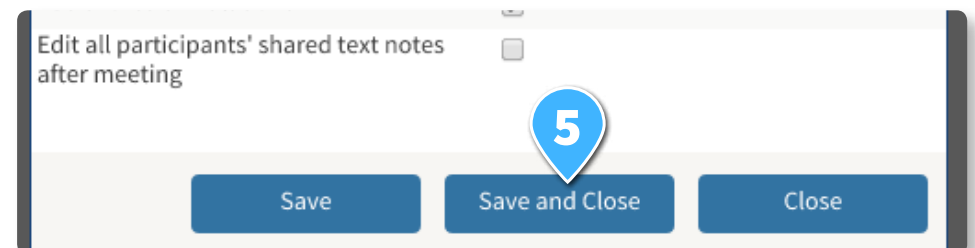
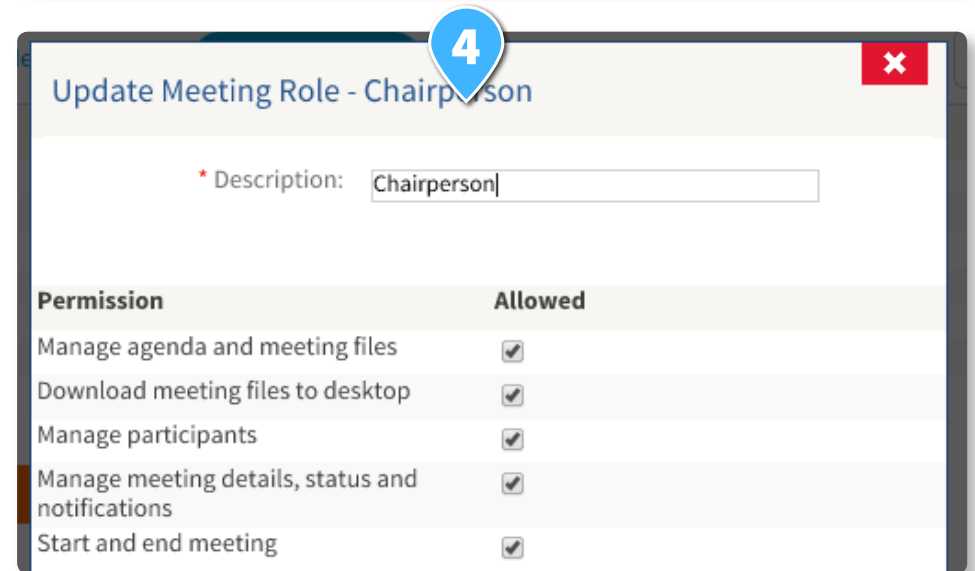
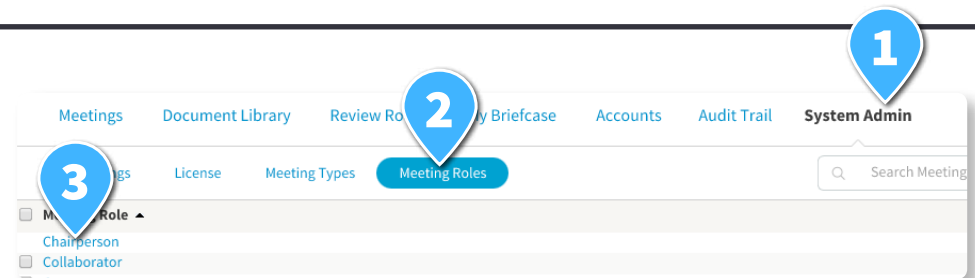
Save **Save and Close** **Close**



Meeting Roles and Permissions

Edit an Existing Meeting Role

1. Click **System Admin**.
2. Go to **Meeting Roles** tab.
3. Select a meeting role from the list.
4. To change what an existing role can do in a meeting, mark or unmark the corresponding checkboxes of function rights listed.
5. Click **Save and Close**.



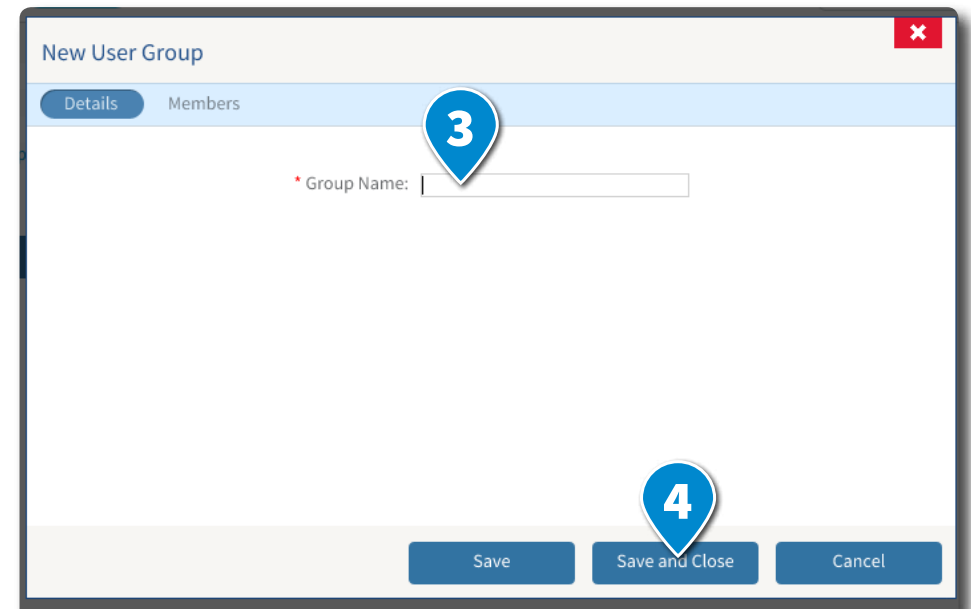
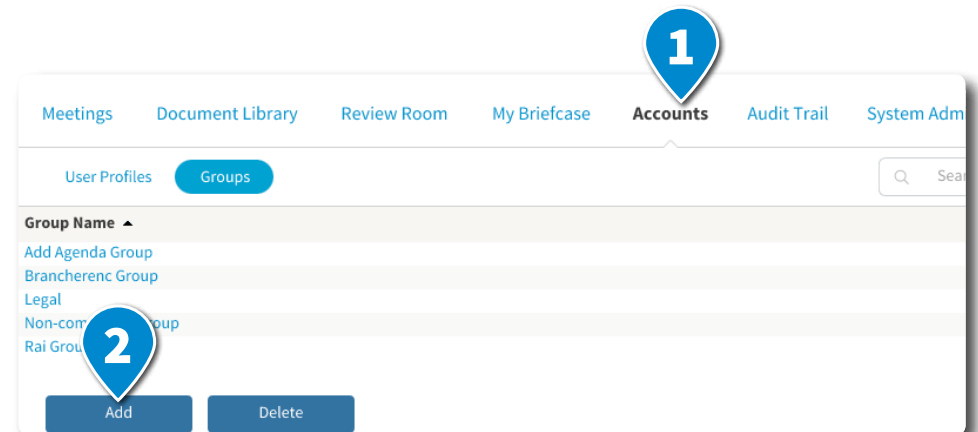


Manage Groups

Convene supports multiple boards and committees to facilitate meeting management and access permissions.

Create a New Group

1. After logging in to the portal, click **Accounts**.
2. Under Groups, click **Add**.
3. Specify the **Group Name**.
4. Click **Save and Close**.





Manage Groups

Add Members

1. In the **Accounts** tab, click **Groups**.
2. Click the group to which you wish to add members.
3. Click the **Members** tab
4. Click **Add**.
5. Select the members you wish to add.
6. Click **Add**.

The screenshot illustrates the steps to add members to a group in the Manage Groups interface. It is divided into six numbered sections:

- Step 1:** The 'Groups' tab is selected in the top navigation bar.
- Step 2:** A group is selected from the list. The group name is partially visible as 'Add Agenda Group'.
- Step 3:** The 'Members' tab is selected within the group details view.
- Step 4:** The 'Add' button is clicked to open the member selection dialog.
- Step 5:** The 'Profile Selection List' dialog is shown, displaying a table of available members. The table has columns for 'Full Name', 'Post', 'Division', and 'Email'. The member 'Nina Lyons' is selected, with a checkmark in the 'Full Name' column.
- Step 6:** The 'Add' button is clicked in the bottom bar of the dialog to confirm the selection.

Full Name	Post	Organisation	Email
Callum Dawson	Legal, Litigation	Dawson Associates International	callum@anywherepad.com

Full Name	Post	Division	Email
Nina Lyons		Solvitech	nlyons@solvitech.com



Manage Groups

Remove Members

1. In the **Accounts** tab, click **Groups**.
2. Click the group to which you wish to add members.
3. Click the **Members** tab.
4. Select the members you wish to delete.
5. Click **Delete**.

The screenshot illustrates the steps to remove members from a group. It shows a sidebar with a 'Groups' button (1), a list of groups including 'Add Agenda Group', 'Brancherenc Group', and 'Legal' (2), and a 'Members' tab (3). The members list (4) contains one entry: Callum Dawson, Legal, Litigation, Dawson Associates International, callum@anywherepad.com. At the bottom, there are 'Add' and 'Delete' buttons (5).

Full Name	Post	Organisation	Email
☐ Callum Dawson	Legal, Litigation	Dawson Associates International	callum@anywherepad.com



Folders and File Permissions

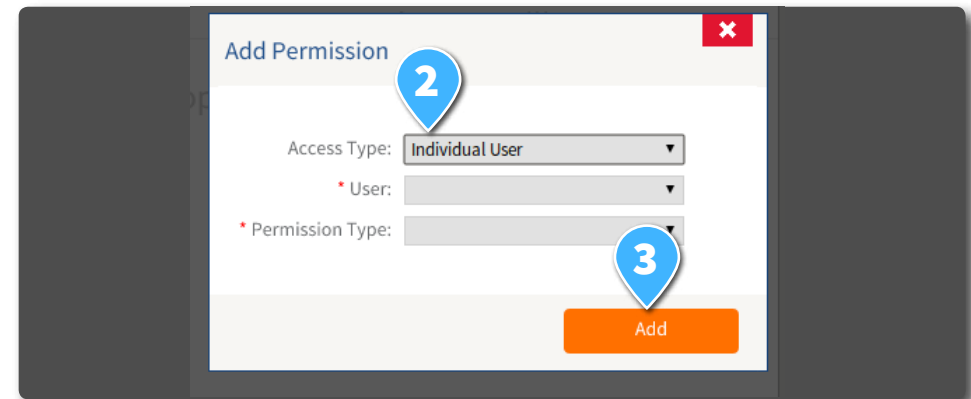
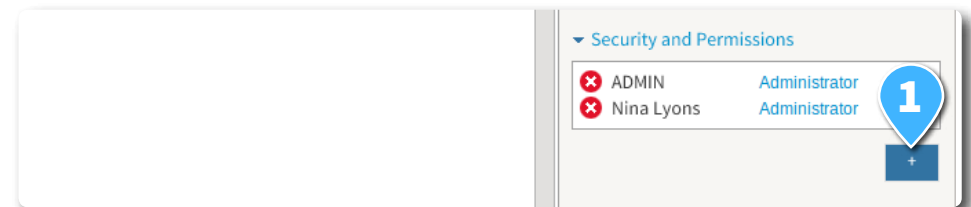
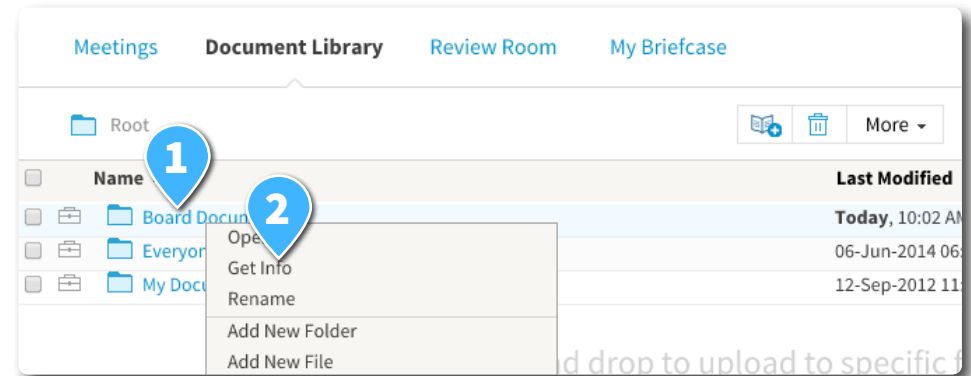
Grant Permissions

Permissions can be managed by users who are administrators of the board, committee or organisation's library.

1. Under **Document Library**, right click on the file or folder whose permissions you want to change.
2. Click **Get Info**.

To grant permissions:

1. Under Security and Permissions, click **+**.
2. Select permission options.
3. Click **Add**.



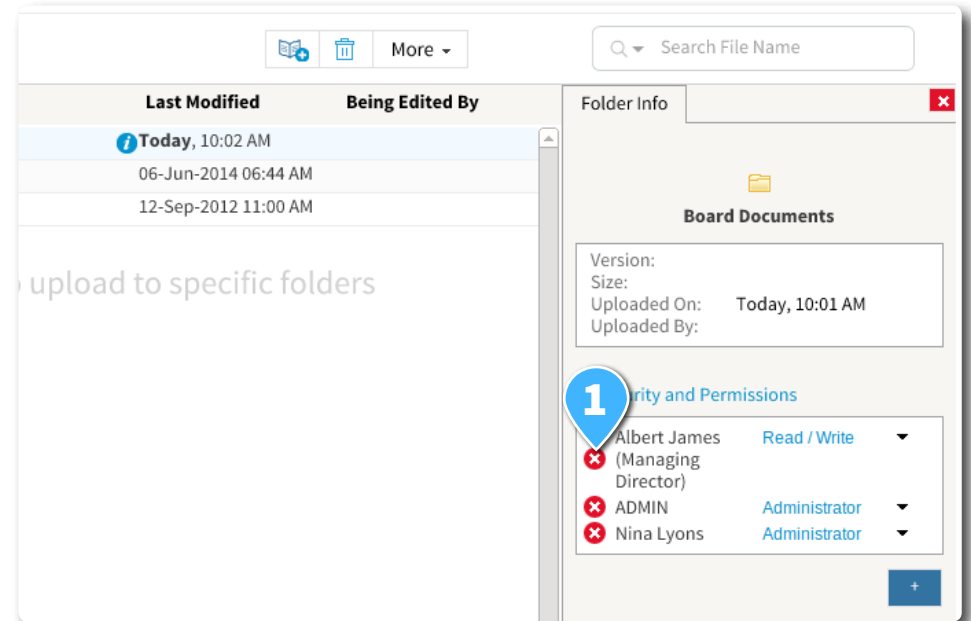


Folders and File Permissions

Revoke Permissions

To revoke permissions:

1. Click **x** on the user whose permission you want to revoke.





Audit Trail

Audit Trail

The Convene web portal's audit trail lets you track the activities being performed within the system. To access the audit trail:

1. Go to **Audit Trail**.
2. Select the audit trail category you wish to view: **Sign In, Documents, Permission, User Profile**.

Category	Description
Sign In	Sign Ins, both successes and failures
Documents	Operations on the files and folders: Download, Insert (new), Delete, Move, New version
Permission	Permissions granted (Insert) or revoked (Delete)
User Profile	Operations on account records



System Administration

Convene lets you configure how the system behaves through the System Admin screen.

1. Go to **System Admin** tab. Under **Settings**, you will see the following options.

Setting	Description
General	
Server ID	Read only field used for debugging
Company Name*	Name of your organisation - this text also appears at the upper right hand side of the portal.
Documents	
Maximum File Size for Uploads (MB)*	Maximum size of each uploaded document



System Administration

Meeting Schedule	
Meetings will be closed after [] hours of the scheduled date and time.	After the specified period, the meeting will become read-only. If blank, then meetings will never be closed.
Enable publishing of meetings*	Allows the meeting scheduler to preview the meeting details before publishing the meeting details to the participants
Send meeting summary*	Send a Meeting Summary file via email to participants of a meeting
Agenda Cover Sheet Default Setting*	Allows the mobile app to insert cover pages for agenda items that have no meeting files
Send email notification to participants when meeting starts*	Automatically send email to participants informing them that the meeting they were invited to is about to start



System Administration

Meeting Schedule	
Meeting Cover Template	Allows the organiser to select a file that will be used as the cover for meeting files
Agenda Cover Template	Allows the organiser to select a file that will be used as the cover for the meeting agenda
Standard Participant Groups	Allows meeting organisers to group participants when scheduling meetings; however, this has no bearing on permissions and is simply an organisational tool

Security Services	
Activate Security Services	Lets you activate the security services or displays the current status if already activated;
Password Expiry	Number of days before passwords expire; when expired, user accounts must provide new passwords when they sign in
Sign-In Retry Limit	Related user account will be disabled and related user offline data will be deleted from the app after retry limit



System Administration

Password Policy

Minimum password length	Sets the minimum number of characters required in a password
Minimum number of letters	Sets the minimum number of letters required in a password
Minimum number of digits	Sets the minimum number of digits or numerals required in a password
Allow special characters	Whether to allow special characters such as ^, &, *, etc.
Disallow reuse of old passwords	Whether to allow users to reuse the last, last 2, last 3, and so on password

Client Devices

Enable automatic sign out after [] minutes	Set the session timeout in minutes
Auto-delete meeting information on sign out	If enabled, cached files will be deleted from the user's mobile device upon sign out or session timeout; offline access will also be disallowed



Manage License

Check License Information

1. Go to **System Admin**.
2. Click on the **License** tab.

Remove License

3. To remove the license, click **Remove License**.

Request a License

4. Click the **Request License** button. It will launch your mail client with a message template that you can send to the Convene team.

The screenshot shows the 'System Admin' interface. The top navigation bar has 'System Admin' highlighted with a blue callout '1'. Below it, the 'License' tab is selected in the sub-navigation bar with a blue callout '2'. The main content area displays the following license information:

- Server Code: [hex string] Click to Copy
- License ID: 2E1F366F-62B1-478C-8CB2-EF24ECFAB5E8
- Licensed Seats: 99,999 accounts
- Registered Accounts: 47
- Remaining Seats: 99,952
- Guest Participants: 3
- Available Features: Review Room, My Briefcase, Resolution
- Valid from: 01/01/2014 to 01/01/2015
- Licensed Storage: 14.4% used (147.84 MB of 1.00 GB)

On the right side, there is a 'Request License' button (4) and a 'Remove License' button (3). A text box on the right explains that clicking 'Request License' will generate a license request to support@azeusconvene.com, asking for the number of accounts to be supported and whether document encryption is required.



Meeting Types

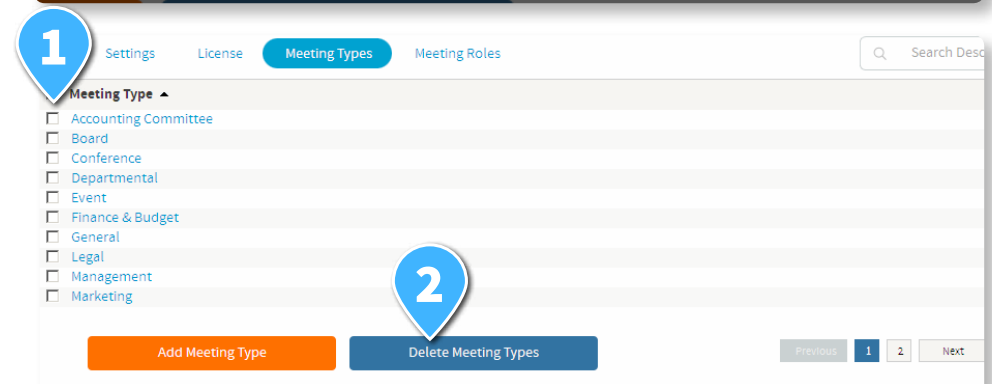
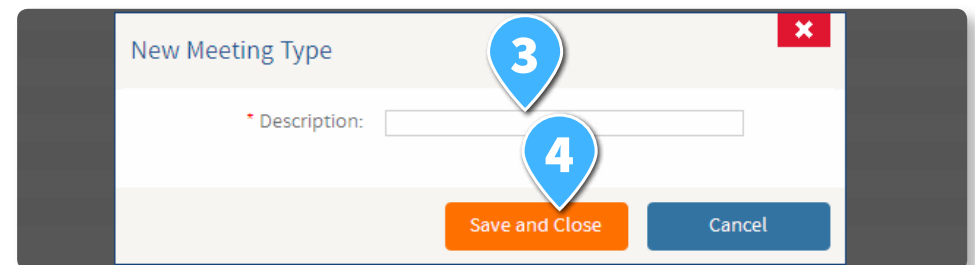
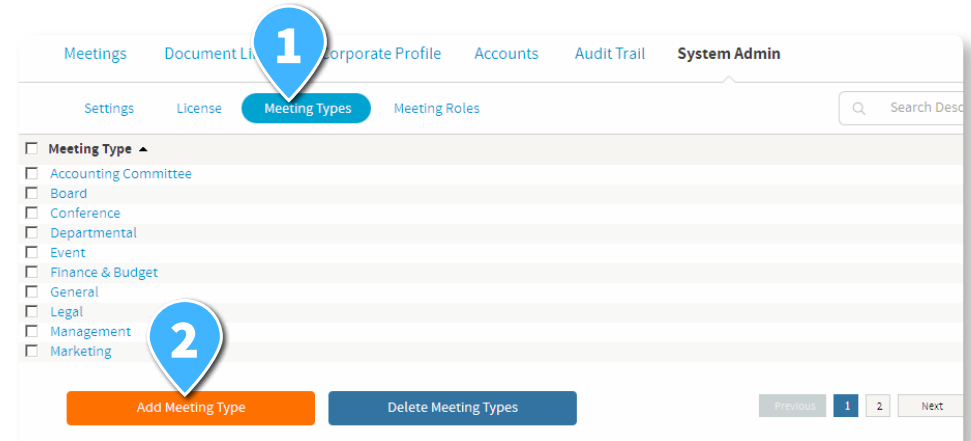
Meeting types allow participants and organisers to easily identify the type of meetings and filter meetings by type.

Add a Meeting Type

1. Under **System Admin**, go to **Meeting types** tab.
2. Click **Add Meeting Type**.
3. Enter **Description**.
4. Click **Save and Close**.

Delete Meeting Types

1. Tick the **Meeting Types** you wish to delete.
2. Click **Delete Meeting Types**.





System Key

System Key

This section is only available if you opted to keep the system key separately (as opposed to storing it in the server).

Safeguard the System Key

The system key is very important because it allows unprecedented access to the service. The system key is able to decrypt user keys, which can be used to decrypt file keys, and thus lets the system key holder access the contents of any document in the Convene repository.

It should be stored on a protected workstation with not just software-related security mechanisms, but also physical security mechanisms.



System Key

Start the Service with the System Key

1. Sign in as **administrator**.
2. Go to **System Admin**.
3. Under **Security Services**, click **Activate**.
4. Locate the private key file provided to you during installation.

The screenshot shows the Convene System Admin interface. At the top, the Convene logo is on the left, and 'Welcome Nina Lyons | Sign out' is on the right. Below the logo is the tagline 'The Boardroom solution, on any device'. A navigation bar contains links: Meetings, Document Library, Review Room, My Briefcase, Accounts, Audit Trail, and System Admin (which is highlighted). Below this is a sub-navigation bar with links: Settings (highlighted), License, Meeting Types, and Meeting Roles. The main content area is titled 'Security Services' and shows 'Activate Security Services: Security services are already active.' Below this are two input fields: 'Password Expiry: 180 number of days' and 'Sign In Retry Limit: 3' with a note '(Related user account will be disabled and related user offline data will be deleted from the app after retry limit)'. The 'Client Devices' section has two checkboxes: 'Enable automatic sign out after 10.00 minutes' (checked) and 'Auto-delete meeting information on sign out' (unchecked). Below the second checkbox is a note: 'Auto-delete all offline documents, meetings and user account information upon sign out or session timeout on Anywhere Pad. Offline access will be disallowed.'